Richard C. Levine, Sc.D., P.E.
Beta Scientific Laboratory, Inc
P.O. Box 836224
Richardson, TX 75083-6224
telephone 214 233 4552
(area code changes from
214 to 972, September 14, 1996)

July 30, 1996

Mr. William F. Caton
Secretary
Federal Communications Commission
1919 M St. NW
Washington, DC 20554

Re: CC Docket No. 92-115
Informal Submission: Rebuttal of Technological
Errors in May 1996 CTIA and AT&T Wireless Submissions
Regarding Rule 22.919

Dear Mr. Caton:

Enclosed is a signed original and 6 copies of my informal filing to the FCC on the above-captioned matter. If you have any questions, please call me.

Sincerely,

Richard C. Levine

Richard C. Levine

enc: as noted

Richard C. Levine, Sc.D., P.E.
Beta Scientific Laboratory, Inc
P.O. Box 836224
Richardson, TX 75083-6224
telephone 214 233 4552
(area code changes from
214 to 972, September 14, 1996)

July 30, 1996

Ms. Michele Farquhar
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M St. NW, Room 5002
Washington, DC 20554

Re: CC Docket No. 92-115
Informal Submission: Rebuttal of Technological
Errors in May 1996 CTIA and AT&T Wireless Submissions
Regarding Rule 22.919

Dear Ms. Farquhar:

Background: I am a telecommunications consultant, and university professor of Electrical Engineering and telecommunications. I was retained in 1995 by C2+, a former petitioner in this docket, to prepare a report on emulated cellular extensions, which was submitted to the Commission on July 7, 1995, and I also attended a meeting at the Commission on July 27, 1995, at which the other petitioners, CTIA and AT&T Wireless Services (AWS), and other participants as well, stated that they had no disagreement with the technological statements presented in my 1995 report. This agreement by CTIA and AWS is significant because my 1995 report directly contradicted and rebutted numerous technological assertions made by both of them in previous filings as the basis of their position. My qualifications as an expert on the technology and operations aspects of cellular and wireless systems were stated in an attachment to the 1995 report.

In May 1996 I saw two additional documents: one filed by the CTIA (dated May 16, 1996) and the other by AT&T Wireless Services (dated May 3. 1996). These documents oppose <u>any</u> changes in Rule 22.919 which would permit alteration or copying of the ESN in a cellular telephone for both extension use (which these two parties have consistently opposed) but also for any other purpose whatsoever, such as replacement of a faulty cellular phone by a repair depot. Soon after, I learned that C2+ was out of business and had agreed, as a condition of settling a lawsuit with the CTIA, that they would drop their petition to the Commission in this docket. After long and careful consideration, I am submitting this informal letter representing only myself and my own views. I have no employer or sponsor whom I represent in this matter.

I am submitting it for several reasons: First, one important effect of a complete prohibition on ESN copying or transfer is to prohibit implementation of the most effective and proven unbreachable form of the industry standard authentication algorithm. This is my main concern, since I have devoted several years of my professional career and my own personal time and expense to developing a truly secure method to prevent fraud, and I am distressed to see its effectiveness diluted due to apparently widespread technological misconceptions and consequent ill-advised actions about the technology of anti-fraud measures. I have no personal or business financial interest whatsoever in the promoting the use of the authentication algorithm, and I have no property rights in the relevant patents or associated technology and am in fact, likely to make more as a technological consultant if I am called on to fix problems created by the continued absence of this technology. I am sadly compelled by the facts to conclude that the present position of the CTIA and AWS, calling for a complete prohibition of ESN transfer, greatly weakens the arsenal of technological capabilities against fraud, and is clearly irreconcilable with their stated motive of fraud prevention. Second, several new false technological assertions are made now by both CTIA and AWS, which require correction so the Commission can reach a decision based on fact. Third, a number of previous false assertions, already rebutted fully in my 1995 report which was agreed to by CTIA and AWS, are again resurrected by them both using different wording. In particular, the most egregious of these false statements arise from a complete misstatement of what I said in my 1995 report about authentication and/or the false claim that emulated extensions have degrading effects or require complex further network development, when the truth is precisely the opposite in several senses of the word. These misstatements of what I said are so severe that, if not promptly and widely countered with the facts about what I said and implied, they could be damaging to my professional reputation when seen by competent people in the industry. Finally, I fear that if I do not speak out, there is then nobody left to speak for the consumer of cellular services who wants multiple cellular phones with the same MIN (directory number). Under the present Rule 22.919, this consumer will be left with only the inferior and more costly MUSDN service offered by several cellular carriers. In fact, from my own point of view, the dispute between the opposing past and present petitioners on both sides appears to be molded more clearly by economic considerations and competition for the "extension" market, than by considerations of preventing fraud.

I am greatly distressed by the CTIA and AWS documents, primarily because the preponderance of the assertions made by both consist of extremely serious technological errors and incorrect statements. These statements are particularly distressing because both CTIA and AWS each have readily available some of the best-informed technological experts in the cellular industry, any of whom could have been called on to make a correct expert statement about the relevant technology. Not all of their technological statements are false, of course, but those which lead to their conclusions are almost all false. Furthermore, it has come to my attention in June that, while these cellular operator petitioners are opposing all exemptions to a prohibition on alteration of the ESN, a large number of cellular operators have been using or encouraging the use of a different type of cellular telephones (the Cellemetry ® system, discussed below) which clearly intentionally violates both the present form of Rule 22.919 and also the previous Rule 22.933. No exemption has been requested by them for this equipment, even though it truly has the potential to produce degradation of the cellular network in some of the very same ways which were falsely alleged by the CTIA and AWS in their prior filings opposing emulated extensions.

I have numbered the technological assertions which I have identified in the two cited documents, and present my comments and rebuttal to each, and then finally my conclusions and recommendations regarding Rule 22.919. I apologize that so much of this material again considers matters already considered in detail in my 1995 report, but this is necessary in several cases to show that many assertions which I respond to here are merely restatements of previously rebutted assertions, which were restated in the cited two letters to appear like a new or non-rebutted facts, when in fact they are not.

1. The CTIA asserts (pages 2-3)that, after 16 months of experience under the wording of Rule 22.919 which became effective January 1, 1995, experience and hindsight have shown that: a) there is no need for the FCC to mandate a requirement for authentication in newly type accepted handsets, because the CTIA is confident that no rule is needed to make authentication available in all (or nearly all) markets, and b) the alleged "adverse affect" [sic., should be "effect"] on manufacturer's repair and upgrade of cellular telephones in the field have not materialized.

1a. Regarding point a): The long delay (from 1991 to 1995) until a policy statement was issued by the CTIA demanding authenticating cellular phones is partially due to a so-called "self-fulfilling prophecy." The 800 MHz cellular carriers were first dubious about the efficacy of authentication, partly because 10 million non-authenticating sets were then already in use, and zero authenticating sets. There were also some persistent technological misunderstandings regarding the specifics of authentication, some of which are repeated by AWS in the recent letter. Since carriers were dubious about its efficacy, they did not unite in demanding that all new sets be authentication-capable. Then, because the number of sets without authentication was growing, the lack of support for authentication continued Finally, in 1995 the vicious circle was broken for the first time and the CTIA deserves full credit that a policy was then introduced to demand authentication capability in new 800 MHz cellular phone introductions. However, this is not an irreversible policy. It is still not a position enthusiastically supported by all member carriers of the CTIA, and many of its member carriers have not consistently supported the use of authentication in the past and have no obligation to do so in the future. This is why the CTIA can only promise that "nearly all" [emphasis added] cellular markets will have it.

Authentication is 100% Technologically Effective, Yet the Cellular Operators are not 100% Convinced: Authentication has been proven by European experience to be 100% effective against technological fraud, but only when it is 100% deployed in all cellular phones and base systems. In contrast, American carriers have tried repeatedly to use anti-fraud methods which are acknowledged to be both highly "porous," (they only identify a fraction of the actual fraud, not all of it) and also have high "false denial of service" rates (they deny service to some valid customers). In contrast, authentication has been proven by European experience to be free of these two faults. During the 5 years since TIA authentication was standardized the population of American cellular phones has grown from about 10 million to about 25 million, and the cellular operators have been delaying a firm decision on the use of authentication, while restlessly flitting from one only partially effective method to another, searching for the elusive "silver bullet" which will consistently deny service to fraudulent cellular phones yet never deny service to legitimate phones. No clear schedule priority was presented to manufacturers of switches and network equipment to roll out authentication in the network, and no concerted industry wide effort has been organized to test and verify network wide compatibility. (The industry can do this when it wants to, as shown by the highly successful "Lockdown" coordinated testing and verification process performed to introduce the IS-54 Digital cellular standards.) Given this history, I suggest that it is essential to protect the interests of everyone (carriers, consumers, etc.) that 100% implementation of authentication in new cellular phones be mandated on a reasonable and achievable calendar basis by the Commission, rather than leaving this to the choice of the cellular operators alone. In my highly biased opinion, this historical delay and indecision has been a major factor in bringing us to the present situation, which has given criminals a long-term free hand to steal service and use cellular phones to further their other criminal enterprises.

Lack of Mandated Authentication Discriminates Against Authentication vis-à-vis Other Anti-Fraud Methods: There is no reason for the Commission to deny any particular possibly valuable anti-fraud technology its opportunity to be applied. Carriers should have the option of using any and all anti-fraud technologies available, particularly when each has its own particular interval of effectiveness or sphere of application. Consider the objections which would be raised if the Commission passed a rule which was prejudicial toward just one <u>other</u> anti-fraud technology. For purposes of discussion, I will mention two apparently useful rule changes which also have adverse effects on fraud control. Imagine the quite valid uproar of objections if the Commission mandated a tight time-domain mask on the cellular control channel frequency shift keying (FSK) signaling waveform to reduce out of channel RF emission, and thereby increase cellular system capacity slightly. Although that ostensible objective could indeed be achieved, this would also have the secondary effect of crippling RF fingerprint or signature anti-fraud technology, since incidental unit-to-unit differences between different sets would also become more subtle and difficult to detect. Similarly, imagine the valid objections if the Commission introduced a rule to limit or restrict the number of digits which could be dialed by a cellular phone following initial connection. This might prevent certain types of conference call dialing errors, but it could also cripple PIN entry as an anti-fraud method. Other examples are conceivable, but all are equally silly, and of course I present these examples only to illustrate that a well-intentioned technological proposal in a complex system like the cellular network can often have unexpected collateral negative effects on combating fraud. In each of these cases, the ostensible benefit of the proposed change must indeed be a <u>very</u> significant contribution to the public interest, convenience and necessity in order to justify the reduction in fraud protection which it produces. I suggest to the Commission that the proposal by CTIA and AWS to not mandate authentication in new set production and to unconditionally prohibit ESN copying or transfer fail this test. Lack of mandated authentication in cellular phones makes ultimate effective use of authentication dependent on the historically demonstrable strongly divided and fickle sentiments of the carriers, and prohibition against ESN transfer prohibits the most secure implementation of authentication (discussed further below). It significantly reduces the best security level of the industry while raising the cost and reducing the quality of service to extension customers, and gives no anti-fraud benefits to compensate for these detriments.

Prohibiting ESN Transfer Prevents the Most Secure Implementation of Authentication: The new position of the CTIA and AWS (now opposing <u>any</u> changes in the ESN) "throws the baby out with the bath water" by consequently forbidding the most technologically secure form of authentication, namely implementation in a separable authentication chip (packaged as a so-called "smart card" or "smart SIM chip"). While the CTIA and AWS are fully entitled to take any position in this debate, including reversal of their position on any point at any time, this particular new position appears to me to be technologically the worst possible position of all for 800 MHz cellular service, since it leaves only the weaker form of implementation of authentication (via combined or "one-piece" software with call processing) available for US use, and is thus clearly inferior to PSC-1900 and other competitive systems with a separable authentication chip. Rapid implementation of the separable chip form of authentication will not only give an unbreachable physical security to the A-key and other secret information, but it will also automatically solve the repair/replacement issue described in the next section, for cellular phones equipped with a separable chip.

1b. Regarding point b): While there is no substantiating supporting data presented by the CTIA for their assertion that none of the concerns regarding set repair and replacement have materialized. I ask for substantiating background information because my own knowledge of the industry indicates that cellular telephone set replacements are still being done extensively via changing the ESN of a replacement set, while everyone concerned merely ignores these violations of Rule 22.919. My impression of the situation may be correct or incorrect, and even if it is correct it does not necessarily imply an explicit conspiracy of silence on the part of anyone. However, if there indeed has been no problem since January 1, 1995, and "business as usual" together with "don't ask, don't tell" is not the true explanation, then one of the following things may have occurred:

1b.1 The reliability of cellular phones has suddenly magically increased so that no repairs are required.

1b.2 A new method of instantaneous repair, not previously reported to the public or to the technologists, has been put in place.

1b.3 Cell phones are being repaired at the normal speed, but customers don't mind being without them for hours to days, and have made no complaints.

1b.4 Cell phones under repair are temporarily replaced by "loaner" phones having a different telephone number (MIN) and ESN, but the customers do not have any objections to the inconvenience of advising all their associates of their new telephone number, and have made no complaints.

1b.5 Cell phones under repair are being replaced by replacement sets coded with the original directory number (MIN) but, of course, having a different ESN than the non-working original set, and are being instantly activated by the carrier without charge to the consumer. This, if it is the reason, is a particularly generous act by the carriers, in view of their prior assertion that the emulated extension customer is merely trying to illegally evade an activation charge for a second cellular phone.

Of course, I propose items 1-2 only in jest and sarcasm, but items 3-4 are only half in jest, and item 5 is quite possible, although it indicates a serious inconsistency in the prior arguments of the CTIA. In any case, I am concerned about the fact that the assertion is made without substantiating background information, so there is no basis for distinguishing between these items, and further concerned because there is no alternate official source for the underlying data. The CTIA may, in fact, be absolutely accurate in stating that it is aware of no complaints and no problems. But if complaints and problems do indeed exist, what guarantee is there that they will reach the CTIA, or the Commission, for that matter? This point is discussed further in the conclusions.

2. CTIA asserts (their page 3) that cloning and emulation are technologically synonymous, and asserts that they involve precisely the same modifications of the memory in the mobile station, and that attempting to distinguish the two via separate names is merely sophistry. This is technologically incorrect and furthermore this incorrect view leads to attacking the wrong problem in the rule. A legitimate extension emulation requires only a change in the 32 bits at the address of the ESN value in the cellular phone's non-volatile memory, and nothing more. (It may be desirable to also retain a copy of the original ESN value elsewhere as a backup to paper records in case the ESN needs to be changed back for later sale or service of the mobile station, but this is not technologically necessary.) A clone may be modified in this way, and this was a common criminal cloning method in the early 1980s when clones were first uncovered. However, today a clone is very unlikely to be modified in such a simple manner. It is much more likely today that a clone will have extensive changes to the call processing software, and in many cases the original ESN is actually not changed. Of course, the clone will transmit an entirely different number value over the air, often a different ESN value will be transmitted each time the clone phone places a call (so-called "tumbling" clone).

Incidentally, as a result of changing only the ESN, an emulated extension may be converted back to its original ESN by anyone with facilities to change the 32 bits involved, and, of course, the value of the original ESN. In contrast, the only sure way to "clean up" a clone, without knowing the precise type and memory address of all the many changes made, is to replace all of the program memory contents and non-volatile data.

Confusion of Emulated Extension with Cloning Leads to a Rule that Could Allow Clones to Evade Prosecution/Conviction: This continued misunderstanding of the technological distinction between an emulated extension cell phone and a typical "modern" cloned cell phone is reflected in the wording of Rule 22.919, which definitely outlaws legitimate emulated extensions in which only the ESN value is changed, but which gives criminals a significant loophole to evade conviction, since many cloning methods specifically do not change the original factory-set ESN value, but only affect the value transmitted via radio by the cell phone. In many cases, the criminal operator of the clone can cause it to transmit the original valid ESN temporarily (via some special keystroke sequences, for example), so that (assuming the MIN/ESN of the clone is assigned to just that person) the criminal has a technological loophole which could allow the criminal to evade prosecution or conviction. After all, the clone then looks and works just like an unmodified set, and a cursory technological examination of the memory will even disclose the proper ESN in the proper place. Of course, a more thorough examination of the memory will ultimately disclose the other cloning changes, but the rule, as it stands, does not make enforcement easier and more consistent. Just the opposite.

CTIA Should Be Aware of this Distinction: The CTIA should have been fully aware of the technological distinction between the simple change of ESN used for emulated extensions versus the elaborate software modifications designed to produce a well-concealed modification of the transmitted ESN value, or a "tumbling" clone, etc., because the CTIA has funded GTE Laboratories in Waltham, Massachusetts, for several years to study the types of software modifications of cloned cellular sets which have been seized in fraud arrests, and GTE Laboratories have prepared extensive reports on this topic for the CTIA.

I give my own suggestion for the preferred wording for the rule, to avoid giving criminals this particular legal loophole, in the recommendation section.

Analogous Cases of Landline and Cellular Extensions vis-à-vis Fraud: The record in this Docket is replete with arguments about analogies between the ESN as compared to credit card numbers, automobile Vehicle Identification Numbers and license plates, and more. Now we have the issue of whether the cellular extension is analogous to the landline extension. The CTIA asserts that both extensions and clones are technologically identical and that both are, per se, fraudulent use as a result of being technologically identical. I have stated above that they are usually not technologically identical internally, and I assert furthermore that they are not both fraudulent, even in the case where they may use the same technology. Since the confusion in the CTIA's case arises partly from considering incorrect analogies between cellular and landline service, I state a comparison, couched entirely in the terms of landline telephone technology, to illustrate that the same technology can be used in a manner which is already well recognized, in that context, as being either distinctly permitted or distinctly illegal, depending upon the status of the user, and not depending upon the technology:

Several years ago, I lived in an apartment house and had my telephone plugged in via a plug and jack (the old 4-prong type) in my apartment. A previous tenant in my apartment had also had had another jack installed in a public accessible basement storage area, connected to my (originally his) particular telephone line at that location. Once I discovered it, this jack proved to be particularly convenient when I needed to make or receive calls while in the basement storage area.

Now consider the following analogous situations:

2.1 When I take my own telephone extension set to the basement from the bedroom and plug it in, I am enjoying use of my own service, which I pay for. This is true with any telephone set which is technologically indistinguishable from my own set. Use of such a set is analogous to cellular extension emulation.

2.2 If another person, without my knowledge or permission, plugs in a technologically indistinguishable telephone set to this very same basement jack, and makes calls which are billed to me, that is fraud and theft of service. Use of such a set (exactly the same type of set as the previous case) is analogous to cloning.

2.3 To say this again in a slightly different way, cellular radio technology is analogous to the jack on my line which is accessible to the public. If I use it, regardless of which telephone set I use or how many telephone sets I own, this is a legitimate extension use and I pay for any measured call service I use. If an unauthorized person uses a technologically indistinguishable telephone set and makes calls with the intention that they are billed to me without my knowledge and approval, this is fraud and theft of service. The fact that both of us use the same technology to connect to the telephone network is not an invariable indication that I am guilty of fraud (cloning) or that the other person is innocent. In fact, the truth is just the opposite.

Furthermore, if I set this scenario in the 1960s, then I would have to pay the local telephone company a monthly recurring charge for each telephone set extension, regardless of whether I plugged it in at my apartment or in the basement. It was not then permitted to buy and own another telephone set which was technologically indistinguishable from the Western Electric brand telephone set rented to me by the local Bell telephone operating company, and plug it into either jack. This is analogous to the situation desired by the CTIA and by AWS, which would be the result of prohibiting the customer from owning a second set which is technologically indistinguishable from the first. Then the only alternative for a cellular customer who desires multiple sets with the same directory number is Multiple Unit-Same Directory Number (MUSDN) service from the cellular carrier, which despite its deficiencies (e.g. no roaming, no alternate A-B carrier coverage at home, etc.) compared to an emulated extension, has a recurring monthly charge which is typically equal to the recurring charge for the first cellular phone set. The various shortcomings of MUSDN service were discussed in detail in my 1995 report and are summarized in the conclusion section below.

Today, in contrast to the 1960s, I can own and use any telephone set meeting Part 68 specifications, and can plug it in to either jack (if I still lived at that apartment), without paying a monthly recurring charge to the telephone operating company. That appears to me to be absolutely analogous to the situation requested by the former petitioners C2+, and others. In that case I can have additional cellular sets yet pay only one monthly recurring charge, and have full capability from any one of my cellular sets (roaming, alternate A-B carrier service at home, etc.).

Air Interface is the Analogous to the CPE Demarcation: I believe that the most technologically consistent position is to view and treat the air (radio signal) interface between the mobile station (cellular phone) and the base radio as the equivalent, in every regulatory way, of the demarcation point in landline service between the customer provided equipment (CPE) and the network provider's equipment, due to the almost identical technological properties of these two interfaces. All other approaches (including the false distinction by the CTIA regarding simultaneous use of extensions on the same channel, discussed below) are technologically inconsistent and appear to me to be a weak attempt to fit the contrary facts into a bad theory.

Further Distinguishing Identification is Desirable and Practical: Although I have referred above to "technologically indistinguishable" cellular phones, I believe that it is advantageous for several reasons (repair and replacement, upgrading, etc.) to have a separate distinguishing identifier from the MIN and ESN for cellular phones with the same MIN,ESN and Authentication A-key, etc. This is described in my 1995 report as well. This is done in the European and related PCS systems by means of a physical equipment serial number (different from the ESN) which can be remotely interrogated under special circumstances. That is one of several methods which are readily adaptable to the US 800 MHz cellular band. Other methods include the use of some of the existing reserved bits in existing call processing messages, or defining certain previously unassigned call processing function codes to identify alternate 800 MHz extension sets, etc. The optimum choice should be set by an appropriate standards committee, where all the parties are represented, although I suggest the first method in my recommendations below merely to give a definite example already proven by European systems.

3. The CTIA asserts (their pages 3-4) that the analogy between landline extension phones and **cellular emulated extension phones is technologically** invalid because they assert that true extensions share one **and only one transmission path linking the various extensions** to the telephone company's end office or network. **The distinction which the CTIA attempts to draw is** technologically incorrect in several ways, or at best a half-truth. **Furthermore, the point is not technologically relevant because** the opposite case of landline station sets exist which also have **identical technological limitations (as claimed by the CTIA)** requiring only one set to be used at a time on a transmission **channel, yet no suggestion has been made** (at least, since the 1960s) that the consumer pay an extra monthly **recurring fee to the landline carrier for such equipment.**

3a. Two or more portable analog handset type cellular phones (all of which have a **pre-existing standard feature called discontinuous** transmit - DTx - a form of voice controlled transmitter switch on or off, **which is designed to conserve** battery power) can indeed be caused technologically to share the precise **same cellular radio channel in the same cell.** Sets equipped with DTx capability are the most popular in sales **and they now constitute the majority of sets** in field use. In a two-set one-channel DTx situation, only one mobile **customer can speak at a time, since simultaneous** speech will cause garbling. However, this is precisely like two **landline extension users coordinating their speaking** so that they do not speak simultaneously, which also causes **garbling. This technological point** of simultaneous channel use by DTx mobiles was extensively investigated **in the TIA standards committee** at the request of the CTIA, among many other proposals to increase the system **capacity of cellular systems in the late 1980s.** It was not technologically developed because, while technologically **feasible, it makes the cellular system operate** as a radio dispatch system (one base station in simultaneous contact **with multiple mobile radios on the same cell RF** channel), which is legally prohibited for Part 22 cellular service. **Therefore, its absence in normal** cellular operation is a legal, not a technical, restriction, which is begging the question **by asking for a legal restriction** based on the existence of a legal restriction, rather than pointing out a true technological distinction.

To give a complete and fair answer, we must say also that, in two particular cases, DTx **operation does not occur.** Some older higher powered vehicle mounted cellular mobile phone sets do not have **DTx capability and always transmit** continuously. Therefore, if two of these were set to operate on the same **radio channel in the same cell, the stronger** transmitter signal (as measured at the base receiver) would dominate **the transmission path and the weaker** one would not be heard (due to the well-known "capture effect" of FM radio). **In addition, some very few base stations** do not have the proper up-to-date call processing software to handle **DTx operation, and they can send a signal** to force all mobile units to transmit continuously (of course, while **running down their batteries more rapidly** as well). Both mobile receivers on the same channel could, of course, simultaneously receive the conversation in non-DTx mode under any circumstances. Therefore, in all fairness to the assertion of the CTIA, there are some cellular mobile sets which cannot share the same transmission channel in the same cell simultaneously, so perhaps we could describe their assertion as a half truth.

3b. The new CDMA cellular mobile sets (TIA Standard IS-95), which are now **undergoing field trials in several cities** and are poised for commercial introduction, share the same **unique single transmission channel between all the CDMA** mobile units in each cell (as many as 64 simultaneously). **The digitally coded speech signals** from all these different CDMA cellular mobile sets are separated by means of their **"tagging" with separate CDMA identification** codes, only after they have been received by one single **common shared base receiver. All the transmit** signals are likewise combined and share one single common base transmitter. **In addition, there are some authorities** who would argue that the IS-54 TDMA mobile sets share the same **transmission channel in the same cell, although** not instantaneously shared.

3c. **In contrast** to the assertion by CTIA that landline extensions are technologically **distinct from cellular extensions** because the landline extensions all access the same transmission path simultaneously **while cellular extensions** cannot, consider the following widely used landline telephone services which cannot operate with **multiple devices** accessing the same transmission path simultaneously:

3c.1. Facsimile machines (FAX)

3c.2. Data Modems

3c.3. Integrated Services Digital Network (ISDN) for voice or data

In addition, each of these devices cannot work properly when there is also a voice telephone **off-hook (in use) on the same line,** even if there is no conversation on that telephone. Many of us have had **the unpleasant experience of a data or fax call** being interrupted due to another voice telephone on the same line **being taken off-hook.**
Each one of these three example landline devices has precisely the same restriction as **cellular emulated extension services and MUSDN** on a single radio channel, namely: The user may own and use **multiple instances of each type of devicew,** so long as only one is connected and powered up on the transmission path **(in this case the telephone wires)** at one time. Attempting to use more than one on the same transmission path **simultaneously will**

produce either mutual interference or a signal from only one will get through, precisely like the case of non-DTx cellular phones.

4. Finally, the CTIA again asserts (their page 4) the claim in connection with the above assertions, that use of emulated extensions must, perforce, be uncontrollable (while, by implication, but never stated by them, the similar MUSDN services offered by cellular carriers are somehow not) and that the use of extension phones will interfere with detection of an actual clone. All of these matters were rebutted in detail in my 1995 report, with which the CTIA agreed without reservation in the July 1995 meeting. I refer the reader to that report for a more complete rebuttal of this claim with regard to both the technological and operational aspects of the alleged interference with fraud detection and enforcement. More discussion of MUSDN is given below in several sections, particularly section 12.

5. AT&T Wireless Services (AWS) first makes a number of legal assertions which I will not comment on, limiting my comments in this filing to only technological issues. In addition, AWS asserts a number of technological problems with improper simultaneous use of multiple extensions (their pages 7-9 and 10-12), but, like CTIA, do not also point out that each and every one of these restrictions on simultaneous use must also be applied to a MUSDN sets as well. AWS complains that the lack of a limit on the number of emulated extensions which a single customer may possess will invariably lead to a high level of false network signals of various types, but Tim Fitzgibbon, attorney for C2+, in a previous letter (Aug. 10, 1995) to Regina M. Keeney, of the Wireless Telecommunications Bureau of the Commission, has suggested rules and procedures to establish a reasonable limit on the number of extensions for each MIN/ESN, which offer I understand is backed by all the emulated extension providers who have appeared before the Commission on this matter. I agree that the Commission should set a limiting number and I give further suggestions in my recommendations section.

"One Free Cloner" Call Argument is Technologically False: In regard to the assertion by AWS (their pages 9 and 10-12) that possible simultaneous emulated extension phone use is uncontrollable, AWS asserts (page 9 and 10-12) that "...there will always be one free cloner call available on the network because carriers will never have the capability of determining whether the second call is a clone or an extension, absent extraordinarily costly procedures to verify usage with the customer ..." This point was fully addressed and rebutted in my 1995 report, which AWS also agreed to in the July 1995 meeting. Without repeating all the rebuttal material on that point, let me indicate that use of a PIN and/or authentication, to give only two examples, are two preferable methods which are both eminently suitable for this particular purpose, and are already extensively available, and which are not – according to the overwhelming majority view in the industry – "extraordinarily costly." None of these anti-fraud procedures and technologies were put in place to address the use of emulated extensions, so their cost, such as it is, cannot be blamed on the presence of emulated extensions. I find absolutely no technological or operational justification for AWS to claim that they must give away "one free cloner call."

Misapplication of Quotation from Levine 1995 Report: In this same section (footnote 21 on page 11) AWS also misquotes and misapplies my 1995 report by applying my statement showing the limitation of using only "velocity" or "time-place" tests in such a case, where the preferred method is clearly use of a PIN or authentication. This misquotation is apparently directed towards making it appear that I agree that there is a higher level of fraud susceptibility for emulated extensions in general. That is untrue, and I did not say that. Rather, I would say that there is a higher level of fraud susceptibility in this case, but only when a carrier chooses to use an inappropriate method of fraud prevention.

6. AWS asserts (pages 9 and 12-13) that "...techniques such as RF 'fingerprinting' which creates a distinct RF profile to validate calls for each phone, will not work with extension phones without significant alterations in the current cellular system – changes again apparently C2+ would have the carrier bear."

Modifications to RF Fingerprint/Signature Systems to Accommodate Extensions are both Simple and Straightforward and Affect Only the RF Fingerprint/Signature Equipment, Not the Cellular Network: The assertion by AWS is technologically incorrect. Furthermore, almost every aspect of the operation of an RF fingerprint or RF signature system which is a part of normal operations and which already exists, is described by AWS as if it were a complex and particularly vexing problem situation caused by emulated extensions and requiring major costly development. For example, all RF signature systems automatically "enroll" new mobile station "fingerprints" the first time setup channel radio signals are received from each particular mobile set in that cell by the RF signature equipment. This is an automatic feature of these systems, and the modification required for emulated extensions is that the RF signature system would require human input in advance to identify the existence of multiple extensions with some particular MIN/ESN values.

Human Input for RF Signature/Fingerprint Activation of Multiple Extension Sets is Actually Less than for MUSDN Sets: In a properly designed RF Signature/Fingerprint system, the relevant part of the human input for enrolling a customer with one cellular phone consists of typing in the MIN, the ESN, and the digit "1" (or perhaps no digit entry) into a data base. In contrast, for a customer with three (for example) emulated extensions, the human input for this case requires typing the MIN, the ESN and the digit "3." For further contrast, the input for enrolling a customer with two MUSDN sets consists of the MIN, ESN and digit "1" for the first set, and then the MIN (same value), the ESN (different from the first) and the digit "1" for the second MUSDN set. All other human input regarding the RF Signature/Fingerprint aspect is the same regardless of the single phone vs. emulated extension vs. MUSDN issue. This is stated in detail to rebut the later claim by AWS that a greater labor force would be required because of alleged vastly greater data entry for emulated extensions. In addition, there is additional input "paperwork" on the part of the carrier for activating a second MUSDN set which is more than the corresponding paperwork for an extension set because the switch produces two billing data record streams for MUSDN sets which must be merged before the final customer bill is printed, never mentioned by AWS.

Handling of Suspected Cloning is Identical for Single Phone and for Emulated Extensions: Today, RF signature equipment indicates a second distinguishable RF "fingerprint" as something special, when it was programmed to anticipate only 1 cellular telephone set with a particular MIN/ESN. In the case of programming for two (for example) extension sets with the same MIN/ESN, the RF signature equipment will indicates a third distinguishable RF "fingerprint" as something special. In both special cases, the RF signature equipment then finds that there is one more cellular mobile set present than it was programmed to find. At this point, other external actions must be taken to determine which sets belong to the legitimate subscriber and which to an illegal clone. Although I will not describe these steps here for reasons described below, further examination of the process will disclose that the rest of the process is identical in both cases. This is not complex problem.

Modifications to RF Signature/Fingerprint Equipment to Accommodate Emulated Extensions is Neither Complex Nor Disruptive: The cross reference of multiple extension phones in the data base is not a new development, and is not complex. It is of the same level of alleged "complexity" as, and must be done in any case, for the support of MUSDN phones. Maintenance and backward compatibility of such a system for existing RF fingerprints already in the system is not complex. Absolutely nothing fundamental about the RF signature systems, nor their existing data storage or methodology, will be rendered obsolete. The only actual significant impact of multiple extensions on an RF signature system will be the storage of the individual "fingerprint" data for multiple phones for an extension customer; one phone for an "ordinary" customer versus two phones for a MUSDN customer. I purposely do not describe here the supporting information to explain in detail why these modifications are not complex and costly for two reasons. First, for reasons of length. Second, to avoid placing in a public document information about the detailed internal operations of anti-fraud systems which could be of value to persons who would abuse this information. This latter point is also addressed in my conclusion section. I will however, give a minimal amount of background to explain why some of the more egregious statements are incorrect.

More information regarding how an RF fingerprint or RF signature system would handle multiple extension phones (and MUSDN phones for that matter) is given in my 1995 report. It is neither complex nor would significant alterations in the RF signature equipment software be required. The assertions by AWS that the cellular network or system would require significant and complex alterations is technologically incorrect for the following reasons:

6.1 The interface between the RF signature equipment is generally (depending upon the design of the RF signature equipment vendor) one of two types. The simplicity of this interface to the cellular network and the fact that no significant modifications of the cellular network are needed in order to implement RF signature equipment installation is one of the major advantages claimed repeatedly by all of the vendors of such equipment. Surely any person involved with fraud control has heard these claims by the vendors. The interfaces are:

6.1.1 A simple "go/no-go" electrical signal to the cellular base station or Mobile-service Switching Center (MSC) to either continue or abort the call setup for the cellular phone being examined by the RF signature equipment, or

6.1.2 A "radio" interface which has no actual wire or data link connection between the RF signature equipment and the cellular network. The RF signature equipment prevents a cellular phone, which it identifies as invalid, from proceeding to set up a call by producing selective radio interference which causes the MSC to abandon the call.

Networking Development Problems Related to RF Signature/Fingerprint Technology is Pre-existing and Not Related to Extensions: In this connection, it is well known in the industry that there are significant technological development problems involved in networking together RF signature equipment at different cells. The problem is even greater when equipment from different vendors is considered. However, one should not confuse this well-known problem between RF signature equipment at different cell sites (which is a basic problem related to the technology of RF signature methodology, complicated by different vendors with distinct proprietary analysis methods requiring different detection parameters) with the problem alleged by AWS of significant alterations in the current cellular system. These problems have nothing whatsoever to do with the presence of cellular extension sets. All new systems go through a development shakedown phase, and these systems are no exception. Furthermore, regardless of the complexity of the eventual development of the networking between the RF Signature/Fingerprint equipment, this has no impact on the cellular network. The interface between these two networks remains as simple as described above.

7. AWS alleges (page 9-10) that authentication technology renders authentication phones unusable in the home area [of AWS's nework, emphasis added]. Further, AWS claims that to accommodate emulated extensions carriers would "...either have to re-engineer the authentication industry standard or perform services for C2+ customers to ensure that their 'cloned' authenticated phones work on the network. Once again, C2+'s proposal is all risk and liability for the carrier and all reward for itself." **Each and every one of these technological assertions by AWS is false.**

7.1 The allusion by AWS to a distinction between authentication in the home area versus roaming is the key to several important technological considerations. It is necessary to give some history here to explain who, what and why. When the authentication algorithm was developed in the standards committee in 1989-91, the question arose regarding whether the standard should require all implementors to place all the secret authentication data on a separate silicon chip with a separate microprocessor, as opposed to implementing it in the same processor and memory as other call processing software (so-called "one-piece"). A separable chip would have been slightly more costly to manufacture (perhaps a difference of one dollar or more), but would have effectively unbreachable security against physical attack (disassembly and electrical probing) on the cellular phone, since the secret information needed for authentication (A-key, etc.) could go in, but will never come out, and cannot be extracted by means of test or measuring equipment! Only identification numbers derived from the internal secret information, and which are furthermore different on each occasion of use and which cannot be used to determine the underlying secret numbers, do come out. Furthermore, optimum security, speed and accuracy in a separable chip implementation would require putting all the identification numbers for the mobile telephone (such as the MIN and ESN) in the separable chip, rather than in the main memory of the cell phone. This is all well proven in the European systems and the US PCS systems derived from them.

7.2 Manufacturers were unanimous in the position that they would not individually increase the cost of their cellular mobile sets compared to others, unless all the manufacturers were mandated to offer the same level of high security afforded by a separable chip, as was already underway in the European GSM cellular standards. The cellular carriers were all represented at these meetings, including in particular the present two petitioners CTIA (with its own appointed representatives, separate from any individual carrier) and AWS (then called McCaw Cellular). The carriers wanted the lower cost of a "one-piece" implementation, and were willing to sacrifice the unbreachable security of the separable chip. Because various scenarios of increased susceptibility to physical attack on the authentication data for a "one-piece" implementation are possible, although difficult to carry out, a call counter was suggested as a remedy by several of the technologists at these meetings. The carrier representatives initially objected to the call counter, or at least wanted it to be totally separate and optional, because they were not sure that the cellular data communications network between the MSCs could update the needed call counter data rapidly enough for the case of roaming cellular mobile sets. The technologists who proposed the call counter pointed out to the carriers that experience indicated that a very large part of their fraud losses occurred with roaming situations, and an optional feature might be too tempting to omit, thus very slightly increasing the susceptibility to roamer fraud. The matter was only settled when the technology experts on the committee agreed to write the industry authentication standard so that the use of the call counter is optional, so any operators who were not confident of the data transmission speed of their inter-MSC cellular data communication links could opt to omit the additional variable identifier.

I repeat this history to point out several important aspects of the industry standard authentication algorithm:

a. The industry standard authentication algorithm, if implemented in a separable chip, has no security need for the call counter. The call counter is included in the authentication standard, as an option only, to improve the security of a "one-piece" implementation against a possible but improbable physical attack on the cellular phone, followed by returning that same phone to normal service in the hands of its legitimate owner without the owner being aware of the success of the attack. Whether optionally used or optionally omitted by the carrier, no change whatsoever in the industry standard algorithm is required to support emulated extensions. No re-engineering (of the network, the air interface, the data bases, etc. etc.) is required. There is no particular reward for C2+ or any other emulator for the network supporting the industry standard authentication algorithm, and no added risk for the operators like AWS beyond what exists at their own explicit request and choice in the existing standard and their own network.

b. The call counter is apparently already omitted by AWS, in particular, for roaming service, where historically fraud losses have been more severe, and is used by them only in the home area, (as accented by my underlining of their quoted text). Given this position of AWS, it is completely inconsistent for them to argue that there is an unacceptable increase in risk for them to support extensions by this industry standard method. Furthermore, even in the home area, AWS has the option of using the call counter for all home customers except extension users, if they so desire. In that way, any alleged greater risk falls only on emulated extension customers, contrary to AWS assertion on their pages 10 and 14. Furthermore, if the wording of Rule 22.919 were altered to permit transfer of the ESN, an emulated extension customer would possibly have available in the near future a separable chip implementation of authentication in his/her cellular phone, thus removing completely the alleged slight extra risk (for both the customer and AWS) arising from the improbable physical attack on the cellular phone.

7.3 AWS asserts (their page 13-14) a chain of technologically incorrect statements regarding the industry standard authentication algorithm and their interpretation of the position of C2+ regarding these points. In the following paragraphs I will attempt to set straight the technological facts and state the correct consequences. **These succeeding factual paragraphs contradict, almost sentence by sentence, the technologically false statements in the last two paragraphs from AWS** on their page 13 and the first paragraph on page 14, with some exceptions as noted.

a. Contrary to the dates given by AWS, the industry authentication standard was completed in 1991. It was available in IS-54 compatible mobile stations within 10 months thereafter. There was indeed a 4 year (or longer) delay before software became generally available for cellular switches, but this was not due to the complexity of the development. In fact, some vendors of network components involved in authentication have not even cross-verified interworking with other vendors to date. The delay in implementation for switches was due primarily to a longstanding state of confusion and indecision on the part of major carriers regarding the relative priority of authentication vis-à-vis other network software developments, combined with a limit on the resources of software development and testing which was available from the MSC switch manufacturers. The carriers did not ask the manufacturers to elevate the priority of authentication software, but did demand other features. There is much more to this story which would be out of place in this context.

b. The industry standard indeed integrates the ESN as part of the algorithm, as AWS states. However, nothing in the industry standard prohibits moving or copying/duplicating the authentication process and related data (MIN, ESN, A-key, etc.) from one cellular set to another. That is perfectly feasible technologically, with no change whatsoever in the algorithm nor in the cellular network. The only prohibition is a legal one, namely Rule 22.919 in its present form. Again, bear in mind that by prohibiting such a transfer, there is a sacrifice of the unbreachable security level afforded by a separable chip implementation. Although this is standard in European GSM cellular technology and derived systems (e.g. PCS-1900), manufacturers are understandably unwilling to put the more costly separable chip implementation into their US cellular set in a competitive market when other manufacturers are not compelled to offer an equally high level of security, and there is no other corresponding benefit such as portability of the authentication to another extension of the same customer.

c. Transferring the entire authentication algorithm in the form of a separable chip (which would include the MIN, ESN, A-key, call counter described above, etc etc) would (contrary to AWS's assertion) cause the destination cellular phone with this transferred information to operate perfectly in AWS's network, local area or roaming or both. Of course, such a transfer is prohibited by the present Rule 22.919.

d. In addition, if we consider a "one-piece" implementation of the authentication algorithm (feasible in most existing cellular sets by modification of the software/firmware) in which there is no attempt to retain the additional variable identifier, two cellular phones having the same other data values such as MIN, ESN, A-key, etc., would indeed operate perfectly on the AWS network out of the home area (that is, while roaming) with no changes in the AWS network. If the option of omitting the call counter was set selectively for emulated extension users only, as previously indicated, there would be complete service for both sets in the home area as well, with no reduction or change in service for non-extension sets compared to the present AWS practices. Although this implementation also is prohibited by the present Rule 22.919, such sets would be highly immune to cellular fraud (to the extent explained before) and would achieve the industry's stated objective of elimination of fraud.

e. AWS asserts that C2+ and my 1995 report argue that the Commission should reject the current industry authentication standard and introduce a different standard, consequently requiring a complete re-engineering of the cellular network to benefit C2+ and penalize the carriers with a large cost. **This assertion by AWS is totally incorrect, both on the factual basis, and it is also a misquote.** I am absolutely at a total loss to comprehend how anyone can read these implication into the previous documents by myself or by C2+. Although I will state my suggestions again in the conclusions and recommendations section, I summarize the relevant ones here to set the record straight immediately on this matter. I recommend:

e.1 Retain the existing industry authentication standard exactly as it now is. Do not make any changes in the implementations of authentication in cellular switches or IS-41 networks. If it is not already clear to the reader, this is completely compatible with the general thrust of my other comments and suggestions and totally contrary to what AWS's accuses.

e.2 Rewrite Rule 22.919 to require manufacturers to incorporate authentication in all new set production, both newly type-accepted designs and, as soon as feasible, continuing production of non-authenticating types which were previously type accepted.

e.3 Furthermore, encourage the production of the most secure form of authentication, namely the separable chip. This would imply that the rule consistently allow specific instances of moving or copying the same ESN into more than one set, when owned by the same valid cellular customer.

e.4 For older sets which can only be practically upgraded via software changes, again permit a specific instance of moving or copying the ESN parallel to the previous case, but again restrict this to only sets owned by the same valid cellular customer. In connection with this last instance, require upgrading the software/firmware in the set as well, for each set having suitable software/firmware upgrade available. All of this is again completely consistent with the present industry authentication standard, without modification.

8. AWS asserts (page 10 and 14-15) that the existence of two extension cellular phone sets with the same MIN/ESN would interfere with the ability of carriers to intercept, to the exclusion of any other communications, the electronic communications of a [targeted] customer as mandated by CALEA. AWS asserts that this would even occur even if a targeted customer used only one of several extension sets at a time. This claim is made without substantiating background information or data. In the absence of any technological reasons to support this assertion, and based on my knowledge of the technology of cellular and PCS systems, I must conclude that this AWS assertion is technologically incorrect.

Again, any possible reasons for AWS's response are beyond my understanding. When a carrier is served with a valid court order to intercept and make available to a designated law enforcement agency the communications of a targeted individual or organization, there is no technological or operational reason why the existence and use of any number of extensions or MUSDN phones by that individual or organization should, in any conceivable manner, impede or affect the ability to completely and promptly respond and provide the requested interception(s). This is also true even in the case (not mentioned by AWS) when the targeted individual improperly uses multiple cellular telephones with the same MIN/ESN simultaneously and even if the base system permitted connection of both conversations.

In all cases, should only persons not covered by the court order be engaged in the targeted intercepted conversation, the operational treatment of this situation will be exactly like the corresponding case in a landline interception. The non-targeted conversations will be excised from the material legally used, and otherwise treated accordingly.

9. AWS asserts 9 specific allegedly costly obligations which would be placed on the carriers as a result of permitting use of cellular extension phones (page 15-16). Without repeating the wording of each of the 9 assertions, I will respond to them in the same numbered order. The reader may need to refer to the AWS document for the corresponding assertion.

9.1 AWS alleges that cellular extension telephones will have improper multiple registration or paging response messages (due to improper simultaneous power-up use) to such an extent that additional carrier staff and resources will be required to handle the resulting situation. Again, the corresponding case of MUSDN simultaneous use is not mentioned. Although the technological details of the two cases are not completely identical, one would assume that the probability of improper simultaneous power-up and consequent duplicate registration or paging response of two MUSDN sets should be approximately the same as for extensions. Therefore, AWS should be put to its proof based on existing MUSDN data to substantiate that the number of such events is sufficient to support this assertion. If no quantitative proof is forthcoming, it is not possible to quantify this assertion, and I can only conclude that the level of such undesirable signaling channel messages is no greater than the level created by MUSDN sets, which AWS and other carriers must find acceptable since they support MUSDN service. See further comments on MUSDN below.

9.2 AWS alleges necessary extensive and costly revamping, due solely to emulated extensions, of the still-unfinished RF fingerprinting or RF signature anti-fraud systems now under evaluation. First, my evaluation of the complexity and cost of the modifications required due to the actual changes required by multiple extensions is clearly vastly smaller quantitatively than those implied by AWS, although no dollar figures have been stated by either side in these filings to date. In my view, the first step in considering such an assertion of high costs associated with an experimental system must be a binding statement by AWS and/or other relevant carriers, once they have completed evaluation and testing, committing them to purchase stated dollar amounts of RF signature equipment for their entire network, not just a few cells here and there. Until this happens, we must view this as a remotely possible but not very probable situation, not worthy of consideration as a meaningful obstacle to the changes in Rule 22.919 which I favor. Once full network implementation of RF signature equipment is a done deal, then it is possible to proceed to examine quantitatively the added resources required by the existence of multiple cellular extension phones, substantiating any claims with hard evidence.

My present view is that the only definite added human interface operational cost for the portion of activation related to RF Signature/Fingerprint equipment is to type the digit "2" (or 3 or 4, or whatever) in the data entry field when a customer signs up for service, and the de minimus cost of an additional waveform data entry internal to the RF Signature/Fingerprint equipment's memory, for each additional operative cellular phone. Surely this does not require hiring extra staff, as AWS asserts. I have the present view that the total additional cost of supporting multiple extensions on RF signature equipment will also be de minimus. However, since it is clearly a minimal additional cost for one set or for MUSDN sets, I see no reason why the multiple extension customer should not pay this minimal extra cost for data memory for each additional set, as was already suggested by Tim Fitzgibbon in a previous letter to the Commission. In short, although I am open to further information which may modify my view, I do not find any basis to justify this as an additional extraordinary or even significant cost for the carrier.

9.3 AWS asserts that industry standard authentication must be abandoned if carriers are to offer service to emulated extensions, a doubly wrong statement covered in detail in my section 7.3.e above. Since it is based on a total misconception by AWS as noted above, it is, in my view, not applicable.

9.4 AWS asserts incorrectly that an existing call (of another extension phone owned by the same customer or of an unrelated conversation) will be dropped or degraded in quality if the extension owner improperly attempts to start another call while the first call is in progress. These incorrect technological assertions were discussed and rebutted in detail in my 1995 report, which AWS affirmed in the July 1995 meeting. Under no circumstances will a properly functioning cellular system drop an existing call of any type because a new call of any type is initiated. Under no circumstances (with the possible exception of emergency overload operational mode*) will a properly functioning and competently operated cellular system block or degrade the service of other customers because of the attempt to setup a call by another phone. Because this assertion is completely false and is based on a false assumption, it is not applicable.

9.5 AWS asserts that some as-yet-undefined new cellular service development is required as a prerequisite to giving continuing service to extension cellular sets. This is false. The present treatment of two sets with the same MIN is well defined and it is this: if one such cellular phone is already engaged in a call, the others cannot begin a call. This applies equally to both extension sets and MUSDN sets. Therefore from the point of view of using this to justify an alleged costly development, it is not applicable.

However, in consideration of the possibility that this statement by AWS may represent a breakthrough compromise action between the opposing sides on this issue, there is also the possibility that it would be desirable for the industry to define some new feature in call processing for extensions. This would, of course, apply to both emulated extensions and to MUSDN equally, since both are presently unable to have two sets participate in the same call at present. For example, perhaps it is desirable that two extensions may be used simultaneously and automatically conferenced in the same call so that their operation would then be more similar to landline extensions. While this is not obviously the desired approach, this matter should be referred to a standards committee for further study.

* In emergency overload mode, certain cellular phones such as a government official(police, military, etc.), designated health care providers (certain ambulances, certain specifically certified emergency care physicians, etc.) or cellular carrier executive's or repair staff's cellular telephone are treated with higher priority than ordinary users. Ordinary users are blocked or restricted in making new calls. The quality of all ongoing calls is not affected. This has absolutely no connection whatever with emulated extension or MUSDN cellular phones.

It is encouraging that a carrier such as AWS is apparently willing to examine the possibility of other types of call handling for extensions and MUSDN sets, and I agree with AWS that other types of call processing which are more useful to the customer are of interest and are worth investigating.

9.6 In responding to this point, I admit that I am not completely sure that I understand the assertion of AWS, and I am prepared to stand corrected if this is so. I take this point to be an objection that there is a resource burden on AWS and similar carriers to respond "immediately" if they have objections to activation of emulated extensions for a particular customer. If this is a correct interpretation of this assertion, then I feel that it is not appropriate I have checked with several sales agencies which market AWS service here in my own Dallas area, and they all confirm that AWS will respond to them within the half-hour for well over 90% of all applications for service, if AWS has any objection to that customer such as bad credit rating, questionable identification or other reasons. Given that AWS is already responding in a time that would fit the word "immediately" quite accurately for most customers today in the normal course of business, it is unreasonable to allege that doing so in the future represents an extraordinary drain on their resources above and beyond what they are doing as a matter of course today.

9.7 AWS asserts special problems to comply with CALEA for emulated extension cellular phones. This assertion is apparently based on a misconception by AWS as described in my section 8 above, and is in my view not applicable.

9.8 AWS asserts extraordinary and/or unpredictable traffic burdens due to emulated extensions. This assertion is apparently based on a misconception by AWS which was rebutted in great detail in my 1995 report, and is in my view not applicable Again, AWS specifically assented to the 1995 report in the July 1995 meeting.

9.9 AWS asserts an extraordinary burden to write customer contracts for emulated extension customers. This assertion is clearly a <u>de minimus</u> cost item. AWS and other carriers have competent full time legal staff members who can, and do in fact, frequently draft a variety of new special customer contract forms without alleging that this produces an extraordinary or excessive internal expenses. Therefore, in the absence of any reason why this contract should be so much more costly to draft than all others, I feel that it is not an applicable objection.

Again, in connection with these 9 points, I feel that it is important to note that AWS incorrectly alleges a number of developments which it claims are required to support emulated extensions, while it does not indicate that the same developments would be required for support of MUSDN. In addition, they completely omit one very important case which cuts the opposite way. Emulated extensions presently work correctly in conjunction with the IS-41 cellular network and thus they can receive proper roaming service throughout the North American cellular network. In contrast, MUSDN secondary cellular phones are incompatible with the IS-41 North American cellular network, since its fundamental architecture is based on a one-to-one relationship between a cellular phone's MIN-ESN pair value, whereas MUSDN sets violate this by having the same MIN in two sets but with different ESN values in the two sets. The high cost of the "wholesale revamping" of the cellular network to support MUSDN cellular phones is nowhere mentioned by AWS, although there would be no corresponding economic cost for emulated extensions since they roam correctly in the North American cellular network already without any new development required.

To recap, of the 9 specific extraordinary operating expenses asserted in this section, I view six of the nine assertions as not applicable due to either a false underlying assumption on the part of AWS, or on an assumed service development effort which does not, in fact, exist. In one case I assume that the cost of providing the response time to activation objections consistent with AWS's present response time is not an extraordinary burden justifying added costs, but I am not confident that I understand the corresponding statement in the AWS letter fully. In addition, most of these items are assertions which were rebutted fully in my 1995 report, which was accepted without objection by AWS in July 1995. One of the remaining assertions is based on assumption which is testable comparison to MUSDN which is discussed further below, and I put AWS to their proof on this matter. One of the assertions is speculative since it involves an experimental system which may or may not finally be widely used in the cellular network, and if it actually used I seriously question the implication of high cost and system disruption made by AWS and ask for their proof. Finally, I view the last item as a <u>de minimus</u> normal cost of doing business. I believe that these items do not justify a claim of huge cost burdens to the carrier.

10. AWS asserts a number of alleged defects in the proposed rules and procedures put forth by C2+ (page 17-18), presumably referring to the same cover letter by Tim Fitzgibbon which I have referenced. Although these are operational rather than purely technological, I feel that it is appropriate to respond to them for completeness and consistency of my message.

10.1 AWS asserts that anyone can clone a phone lawfully under the rules proposed by C2+. My understanding of the specific procedural and operational methods proposed by Mr. Fitzgibbon to be used by vendors offering extension service, would prevent unrestricted use of the equipment by mandatory use of encrypted transfer, central data bases, and other well-proven methods which appear to be technologically superior to the purely "locked door" and "erase before write" protective methods used by the authorized repair depots of the manufacturers. I agree that totally unaccountable changing of ESNs by anyone, anywhere, is not in the public interest and that adequate controls should be in place to prevent this, but I believe that the rules and methods proposed by Mr. Fitzgibbon are adequate for this purpose.

10.2 AWS asserts that the emulator would not be held accountable for mis-instructing the customer or other errors. Again, my understanding of the procedures proposed by Mr. Fitzgibbon did not unfairly protect the emulator from just responsibility and accountability for any errors, omissions or wrongdoing, and I agree that all parties involved in the process should be held properly legally responsible for their proper actions.

10.3 AWS asserts that the procedure proposed for notifying the carrier of emulation is a "license for subscription fraud." Again, my view is that the emulator is following the same steps as the carrier or the other sales agents of the carrier to verify that the customer is properly identified and is a valid customer of the carrier. Furthermore, under the procedures proposed by Fitzgibbon, the emulator gives the carrier written notice so the carrier can respond if there is any perceived problem regarding this particular customer, who is, significantly, already known to the carrier. I cannot find why this is a "license for subscription fraud," when the existing procedures of the carrier's own present sales agents are the very same.

10.4 AWS complains that the proposed procedures place the entire burden of the carrier to police the system for simultaneous registrations, but objects that there is a dispute about the number of such simultaneous registrations which is likely to occur. First, in direct response to the stated question, AWS is quite naturally assuming that only the carrier will monitor the use of the radio channels, because this is an ongoing result of operating the cellular switch, which stores all manner of historical message and traffic data in the normal course of business. I must agree that everyone is looking to the carrier for this type of information because the carrier produces it normally. In fact, if my suggestion (in section 13.a comments below) to restrict monitoring of the cellular setup channel were codified into law, a third party would need to justify any monitoring of the setup channel, even if the purpose were only to gather independently the information already gathered by the carrier. At another level, this leads to some additional significant questions which I will take up in the conclusions.

As this particular allegation is once more based on the stated assumption by AWS that improper simultaneous extension use will be frequent and uncontrollable with emulated extensions, but no mention is made of the comparable incidence expected with MUSDN, I will take this point up again in my comments on MUSDN in the conclusions.

11. **BellSouth Cellemetry ® and its Relevance to Rule 22.919:** Appendix A is a brief summary of a technology developed and owned by BellSouth Wireless, Inc. As the summary explains, this technology uses existing cellular networks to transmit remote measurements (traditionally called "telemetry") via the cellular network, to a "home" data base connected to a "home" MSC. A typical application of Cellemetry ® is to send a signal each time an item (such as a can or bottle of soft drink) is dispensed by a vending machine in a remote location, so that the owner of the vending machine will know when to restock it with product. Transmissions from the Cellemetry ® CRAD cellular phone can also be initiated periodically by a clock mechanism instead of as the result of an unpredictable event. To my current knowledge, this technology is already in use in the service areas of many different cellular operators. Operators charge the end users a fee for use of Cellemetry ®, in addition (in some cases) to providing the Cellemetry ® CRAD cellular radio equipment used at the remote locations.

11.1 First, I must say outright that the technology involved in Cellemetry ® is novel, audacious, and intriguing, and is an admirable invention for effectively utilizing the existing cellular network to provide a data communication link. My purpose in bringing Cellemetry ® into this discussion is not to hinder its further appropriate use and development. In fact, I will propose particular exceptions within Rule 22.919 in my conclusions to ensure that Cellemetry ® can continue to operate legally. At the same time, based on my technological analysis of the Cellemetry ® sytem, I disagree with several of the claims made in Appendix A, and I have great concern that the development of Cellemetry ® has several significant implications regarding the present dispute about Rule 22.919.

11.2 Based on my past detailed analysis of cellular setup channel capacity constraints, and my understanding of the Cellular system, I disagree with the second sentence of page 1 and the top paragraph on page 3 in Appendix A, which claims that "at no time does the Cellemetry ® system impose any significant capacity restraints on the cellular telephone system." Without repeating all the reasons in detail, the algorithm for control of Cellemetry ® transmission requires that the setup channel be "quiet" for a specified time before the Cellemetry ® CRAD cellular radio will transmit. However, no device can predict the future, and there is no way to prevent ordinary cellular radios from also trying to transmit at the same time as the CRAD, regardless of the presence of a prior quiet interval. In a typical situation in which there are highs and lows of setup channel traffic, there will be peaks of ® CRAD cellular radio setup channel transmissions after each interval of "quiet" on the setup channel. This can cause repeated "collisions" with ordinary cellular phone call processing messages, leading to delays before the cellular phone can try again, and in the most serious case, to aborting the initiation of regular cellular phone calls in that cell as a result. Furthermore, the CRAD transmissions are controlled by an internal clock or by an unpredictable event, rather than by the normal timing control parameters which are broadcast by the cellular base station. Therefore, to a certain extent, the carrier does not have the type of control over autonomous registration messages from the CRAD which the carrier has over ordinary cellular phones. All this leads to a setup-channel traffic impact, and a number of related questions regarding the assertions by the CTIA and by AWS in the current proceedings, and their prior allegations regarding alleged impact on the performance of cellular systems by such alleged problem situations as multiple registrations or other setup channel signals from emulated extensions. Although I was under the impression that these allegation had been adequately rebutted in my 1995 report, they have surfaced again in the form of the various current allegations by AWS that there will be uncontrollable multiple registration messages from multiple extension cellular phones, and various dire consequences arise from that which lead to complexity and expense in the network, need for staff and other resources, etc.

While I do not want to exaggerate the level of problem which can result, it is significant to note that Cellemetry ® equipment can in fact be truly responsible for the very type of multiple registration and other setup channel activity which AWS incorrectly asserts are deleterious aspects of the use of extension telephones (but which I contend would only happen with improper simultaneous power-up of multiple extensions). There is no coordination between different installed Cellemetry ® CRAD cellular radios, and there is no way to prevent several of them in different locations from sending a registration message simultaneously. Even in the case where the timing of the Cellemetry ® CRAD cellular radio's transmission is controlled by a clock, it could interfere with setup channel signals from ordinary single cellular sets, since there is no coordination between the two. I fully recognize that the potential problem with ® CRAD cellular radios can be minimized by carefully coordinated placement of these devices, but great care must be taken to limit the number and placement of ® CRAD cellular radios in each cell or sector, based on their expected traffic, to try to control this adverse effect on the setup channel. If CRAD placement is done without great care, a problem can indeed result.

One preferred implementation of Cellemetry ® is to use the same "fake" MIN for all the Cellemetry ® CRAD cellular radios associated with a particular cellular operator, regardless of their installation location. As a result, they will all produce IS-41 network messages back to the same home MSC, without using up all the allocated telephone numbers for that MSC or duplicating MIN values assigned to real customers. Therefore, their appearance to the network and base stations is like a flock of un-coordinated cellular radios with the same MIN telephone number, which could often all simultaneously send registration messages on the setup channel. These are the precise things which AWS in particular objected to and claimed would be a major problem with emulated extensions. It is then significant to inquire why the same type of multiple registrations are so objectionable to the carrier when they are produced only by improperly simultaneously power-on emulated extensions (and thus their quantitative occurrence is a matter of dispute, requiring a mistake by the customer), but the same type of signals are strangely acceptable to the carrier when they are produced by <u>normal operation</u> (not a mistake in their use) of equipment for which the carrier receives extra revenue, or for that matter, when they are produced by the same type of mistaken simultaneous power-on of two MUSDN sets.

11.3 One of the most important relationships of Cellemetry ® to the discussion of Rule. 22.919 is that a Cellemetry ® CRAD cellular radio can only perform its intended function by intentionally and repeatedly violating Rule 22.919 each and every time it transmits. Its very existence is a violation of the rule, since the ESN value in memory is constantly changing. Not only that, but it also intentionally violates the predecessor rule 22.933. This is a result of the fact that the ESN in its memory and the value transmitted by the CRAD cellular radio is <u>not</u> a fixed value set at the factory, but is in fact a variable such as the number of soft drink cans remaining in a vending machine. Under certain circumstances, when all 32 bits represent the telemetry data value for example, there is no way to prevent two or more CRAD cellular radios from producing the same MIN/ESN values in their unrelated (and possibly nearly simultaneous) registration signals on the setup channel. Apparently the cellular operators do not object to this.

Clearly, the Cellemetry ® CRAD cellular radio requires a specific exemption in Rule 22.919 in order to operate legally, and I believe that such an exemption should be included in the rule to permit the valid operation of this device and others like it which perform a useful function and which, when properly and competently provisioned in the system, have a small but not overly deleterious effect on the cellular network. If the cellular operator is willing to tolerate the amount of uncontrollable setup channel traffic produced by a reasonable number of installed CRAD units and there is not an unjust amount of system degradation which would affect the ordinary cellular customers of the system, then the operator should be permitted to get the extra income arising from the installation of the CRAD cellular radios. However, for consistency, the operator should not then be allowed to selectively assert objections to other types of equipment which, only in the case of serious improper use, would produce precisely the same types of signals as the Cellemetry ® equipment. Particularly when these devices such as emulated extensions and MUSDN extensions do <u>not</u> produce any extra setup channel messages when used properly.

11.4 Related non-technical Issues. Aside from the purely technological issues related to Rule 22.919 which are involved in the use and operation of Cellemetry ®, there are some non-technical issues relevant to the current dispute which must be considered at this point.

To my knowledge, the very existence and the widespread use of the Cellemetry ® system has not previously been brought before the Commission in connection with Rule 22.919 by any other party to this docket, despite its obvious relevance. I only learned of its existence and its means of operation in June, although I was aware before that that BellSouth and other carriers had a telemetry system operating via the cellular network for more than a year prior to this, and possibly longer. Before that I assumed it used a traffic or voice channel. BellSouth has apparently made extensive presentations seeking to license this technology to other carriers, and has in fact negotiated several such licenses. Therefore all the cellular carriers such as AWS, and likely the CTIA as well, should have been aware of Cellemetry ®. Assuming this is true, it is necessary to raise the question of why neither they nor any other carrier ever came forward to request an exemption from Rule 22.919 or its predecessor rule so that Cellemetry ® could be legally installed and operated.

Some proponents of the Cellemetry ® system have claimed that Cellemetry ® CRAD cellular phones should be automatically exempt from the old Rule 22.933 and the new Rule 22.919, and furthermore they argue that the proponents of this technology have no responsibility to bring this item to the Commission to request an exemption, because a CRAD generally does not have voice channel capabilities and would not respond to a voice channel assignment command signal from a base station, if such a signal were transmitted. I disagree. There is no excuse for this in one special case when another case is being contested. CRAD radio units all have the ability to scan the various radio channels, since each cell uses a different channel for setup purposes. They must meet type acceptance emission masks to prevent harmful interference to other cellular radios. It is well known that the emission mask for FSK setup channel transmissions have more adjacent channel emission than voice channels do, and the injudicious geographical placement of a CRAD unit could cause interference with all mobile unit call setups or paging responses from that cause alone, aside from the possible co-channel simultaneous transmissions described above. To permit the legal operation of Cellemetry ® equipment, there must be both a specific exemption in Rule 22.919 and also a prohibition against manufacture or alteration of a Cellemetry ® CRAD set so that it could use a voice channel or even interfere with a voice or traffic channel in any way. To do otherwise is to open yet another technological loophole for criminals to evade prosecution. In addition, if there is interference with call setup of ordinary cellular phones from this cause, either due to co-channel or adjacent channel interference, the ordinary customer normally has no way to learn that the cause of bad service is because the carrier has permitted too many CRAD units in one cell. This point is related to the question raised in the following paragraph. Given adequate controls on the provisioning, setting of timer controlled transmissions, etc., however, it is likely that a properly sized group of CRAD units in a cell can do its telemetry job effectively with only minimal effect on the setup channel.

11.6 The topic of Cellemetry ® also again raises the related questions regarding who is responsible for observing the proper use of the cellular band, and what motivation each involved party has to bring all the relevant information about its use before the Commission.

12. **Conclusions:** Clearly the Commission has been historically moving from a past "micro-management" policy of the carriers to a future non-directive policy in which licensees will be given a very free hand regarding the technology of radio band use, and competition rather than detailed regulation will be the basis for control of prices and services offered. I support this and view it as a positive method to increase innovation and use the Commission's resources more effectively. However, in several ways (which I have alluded to before) the carrier "holds all the cards," and when forces of competition alone, given the limited number of competitive carriers, do not produce the best service at the lowest fair and compensatory price, the Commission must still investigate and act in such matters and set them right if the facts merit this. In this particular case, my information is that some carriers have tolerated emulated extensions in the past to varying degrees and some have not, but that recently, and particularly when MUSDN was offered by a carrier in a particular market, aggressive action was then taken by both carriers to prevent and remove emulated extensions, and the consumer had no competitor to turn to in that market.

The Commission's view of what is happening in the cellular and PCS industry should not be molded by the vision of only one party; neither the carriers nor by adversaries. But when disputes arise, the carriers are often in a unique position of holding the necessary information. For example, cellular carriers produce all the operational data regarding the cellular system, in the normal course of business, on magnetic disk or tape as an automatic byproduct of operation of each MSC. When a cellular carrier makes a claim such as "excessive simultaneous registration messages will occur with emulated extensions," that carrier is in a unique position of having the data to either substantiate or not substantiate the allegation, and should be obliged to either present the supporting data or just not make the unsubstantiated claim. More on this point below. Similarly, when an adersary needs such data to refute or disagree with the carrier's position, the carrier should be required to produce it under appropriate controls to protect the legitimate interests of the carrier. This also applies to operational information not produced by the MSC, such as the CTIA claim that no problems have materialized regarding repair or replacement of cellular phones since January 1, 1995

In another type of issue, if a carrier raises the objection that a certain proposed change in the rules would have an adverse effect on a proposed anti-fraud method which is under evaluation by the carrier(s), then it is necessary to have some factual information placed before the Commission regarding the efficacy of the proposed method and the likelihood that it will actually achieve widespread use. Without this information, one is entitled to a certain level of skepticism regarding whether the carrier is sincerely concerned about interaction of the proposed rule change with the proposed anti-fraud method. It may be that there is no serious plan by the carrier to use the proposed anti-fraud method, but it merely serves as a convenient basis for arguing against the adversarial position. For example, in this filing, I have asked that the carriers make a firm commitment to actually install and use a particular anti-fraud method in their entire system as a precondition to continued discussion of that particular method in this controversy. I specified the "whole system" because, in this case, the carrier's objection was that the problem related to the overall networking aspects of this anti-fraud system. Now, in all fairness to the carrier, the evaluations may be at such a preliminary stage that, while the proposed anti-fraud method is now promising, it is not yet reasonable at this stage to make a business commitment to it. In such a case, the carrier should be required to present the relevant performance data available from testing (not merely claims by the vendor of the proposed anti-fraud method). The Commission's own staff can then draw their own conclusions about how seriously to consider the proposed method. For example, if a proposed anti-fraud method allows 20% of the actually fraudulent calls to get through, and incorrectly blocks 10% of all valid calls placed, then I believe that a reasonable conclusion is that it is not acceptable for general use. Conversely, if another anti-fraud method allows only 1% of actually fraudulent calls to go through, and incorrectly blocks only 1% of all valid calls placed, then this margin of error is within the 2% blocking grade of service required by cellular systems, and this level of technological performance qualifies this second example system for general use. Judgments of this type must, of course, also be tempered by the cost of the proposed system, since some systems are very accurate but are also very costly and, particularly if their cost is greater than the losses they are intended to prevent, they are therefore not likely to be acceptable for general use. Therefore it may also be appropriate for the carriers to place before the Commission relevant cost and current fraudulent loss data as well as purely technological data. Naturally, all of this type of sensitive information must be protected from view by the general public, by competitors and possibly also, in certain cases, by the adversaries in the hearings, via a suitable sealed submission procedure so the sensitive information is examined only by the Commission staff.

As a non-attorney speaking to a group of legally experienced readers, I recognize that I may well be "reinventing the wheel" with regard to these conclusions about procedural and evidentiary topics. However, from my own technological and non-legal point of view, this docket appears to be particularly heavily clogged with non-issues which have been elevated to the status of issues due to the lack of necessary correct factual information or data, and a large amount of paper and time could have been saved if all parties were obligated to only present technologically substantiateable or substantiated data.

Comments on MUSDN: This carrier service is so intertwined with the issue of emulated extensions and the various objections to it that it requires special comment.

MUSDN is actually <u>not</u> a cellular network technology. It is just two separate cellular telephone sets which have their MIN value set to the same number. The two billing data records are merged in the billing process (in some cases by means of a secondary "off-line" billing software system) to present a single bill to the customer. In fact, as mentioned earlier, the fact that two MUSDN cellular phones have the same MIN but different ESN values is fundamentally incompatible with the North American IS-41 cellular network. Consequently, a MUSDN customer can only use the primary cellular phone while roaming. The second MUSDN phone will not work while roaming. Even if there are bad radio coverage areas in the home city of the MUSDN customer, the secondary MUSDN phone will not automatically switch over to the alternate carrier in that area (of course, assuming that the competitive alternate carrier <u>does</u> have adequate radio coverage in that particular area of the city, which in fact is often the case) as an ordinary cellular phone or an emulated extension or the primary MUSDN phone will do. This problem with MUSDN sets is not impossible to overcome by means of a "wholesale reworking" of the North American cellular network, but this will be a long term and very costly development process, particularly costly in view of the relatively small market penetration of MUSDN. Emulated extensions have none of these shortcomings, since either set will work both at home and when roaming, using the alternate carrier, etc.

Both emulated extension phones and MUSDN phones have the limitation that they cannot be powered up simultaneously, because they will both respond to paging messages (paging messages use only the MIN – not ESN -- to locate the cellular phone) and produce other simultaneous or near-simultaneous messages to the cellular network on the setup channel, such as autonomous registrations, etc. At present the call processing treatment is uniform for all makers of MSCs. Only one of the two (or more) sets with the same MIN (whether MUSDN or emulated extension) can have a cellular call at a given time. Once one set is engaged in a connection, the other one cannot begin or answer a call. This could also be change by means of new software development, but first there must be a definition of what the desired behavior of two such sets should be, which is accepted by the industry and approved by an appropriate standards committee. I must emphasize that this applies equally to both MUSDN and to emulated extension sets.

Both emulated extension and MUSDN cellular phones (if both sets with the same MIN are improperly left in a power-on condition simultaneously) are able to cause certain problems to the cellular network and to the "velocity" or "time place" anti-fraud methods. AWS, CTIA and other carrier petitioners have repeatedly claimed that customers will not be able to properly prevent the simultaneous power up condition of multiple emulated extensions, but at the same time, they do not give any credible reason (or in fact any reason) why MUSDN customers would not be equally likely to leave multiple sets in a power-on condition just as often as emulated extension owners. Rather than just argue endlessly about this issue, I would like to propose that some substantiating data be put forward on this topic, and if it is not forthcoming, I suggest that the allegation of extraordinary simultaneous unwanted setup channel signals no longer be considered in these deliberations. To produce substantiating data, first, the carriers are in a unique position to present real data from the so-called "stats" produced in the normal course of business by the MSCs under their control. They can present the actual counts on the number of occasions in which MUSDN customers have improperly left multiple MUSDN cellular phones (which they can already unambiguously identify) powered-on simultaneously, thus leading to simultaneous paging responses, autonomous registration messages, and the like. The data should be drawn from a number of different markets and cells in a number of different calendar months in accordance with good statistical sampling criteria. This data can be compared to the number of MUSDN customers in each such market to determine the rate of such mistakes by MUSDN customers (the rate being the ratio of the number of erroneous messages per month per MUSDN cellular phone). It appears to me that this number is a reasonable basis for extrapolation to determine how often to expect similar errors by emulated extension users as well. If the carriers have good reasons to present which would indicate that the expected rate for MUSDN users is different from emulated extension users, let them present their reasons and let the Commission evaluate them. If there is a concern that the carriers would be releasing proprietary competitive information in this form, let them present this data only to the Commission and not to their adversaries in the hearings. I trust that this will put the discussion on a quantitative and factual basis, rather than continuing on the basis of repeated qualitative accusations, rebuttal, acceptance of the correctness of the rebuttal, and then the same accusation repeated all over again.

13. **Recommendations**: My recommendations in this section are merely an abbreviated summary of a few of the many specific proposed revisions with comments and explanations contained in the previously noted August 10, 1995 letter (and its attached exhibits) from Tim Fitzgibbon to Regina M. Keeney of the Commission, highlighting only those portions which bear on the specific points in the previous rebuttals of this letter. I earnestly refer the interested reader to Fitzgibbon's letter for more details and explanation. Regarding the specific subject of Rule 22.919, I suggest that the Commission modify that rule to address the following considerations:

13.a A general prohibition on modification of the ESN should be so worded that each mobile station should be manufactured with a unique ESN value, and any modification which makes the cellular set *capable of transmitting* an ESN value different from that set by the manufacturer is prohibited (with only the following specific 3 classes of exemptions: d, e and f below), rather than a narrow prohibition which only prohibits changing the ESN value in memory.

Comment: Wording which only prohibits changing the ESN in memory will give a criminal a loophole to evade conviction, by use of a mobile station which has been modified in such a convoluted manner that the original ESN is untouched and still resident in the proper memory location, but a knowledgeable criminal user can cause the set to selectively emit a different unauthorized ESN value. That emission is what allows the cellular phone to identify falsely for purposes of billing fraud, not the nominal value of ESN in the memory.

It is also desirable that coordinated steps be taken in other areas of the law to, for example, possibly make import, or possession (in addition to use) of a set which does not meet the provisions of this rule, and its explicit exceptions, an offense. Rules prohibiting monitoring the setup or voice/traffic channels to "harvest" of ESN values off the air for fraudulent purposes are also desirable, although they have no logical connection with the way a cellular phone transmits its ESN value or Rule 22.919. Such additional laws are clearly beyond the scope of this Docket, but would be significant in a properly organized legal program to apprehend and prosecute criminals.

13.b I strongly recommend that the Commission rules do not mandate encoding or splitting the ESN in memory in any particular way, or splitting the ESN into non-contiguous pieces in the cellular phone memory. Crooks know how to defeat this, by running a "program trace" on one sample set of the same manufactured type, and after that there is no secret anymore, and there is no protection afforded by special coding or splitting. Leave the implementation details of how the ESN is stored in the cellular phone to the design discretion of individual manufacturers.

13.c Authentication according to the TIA standard should be a requirement, as soon as it is feasible, for all new type approved sets for 800 MHz band cellular service. Authentication, even in a "one-piece" implementation, is so much more secure than use of a non-authenticating set that it should be mandatory because of its value to the industry. Because a "one-piece" implementation of authentication is easy to add to the software/firmware of a design already frozen in hardware form, it should be permitted, but nothing in the wording should prohibit the use of the even more secure separable chip implementation.

Comment: In addition to the specific measures mandated immediately by proper wording of the rule, as noted in the previous paragraph, I also suggest that the Commission should take all appropriate steps to encourage and promote the use of the most secure separable chip implementation of the authentication standard. A working group with representatives from carriers, manufacturers, and consumers should confer with all affected parties to arrive at a practical yet early date for mandatory separable chip implementation of authentication, as well. As discussed in section 7.2, manufacturers will most likely make this secure implementation once it is mandated, rather than being left as a competitive issue with cost penalties to the innovators of fully secure cellular phones.

In addition, to fill in the remaining gap, I most strongly recommend that, as soon as it is feasible (after consultation with the parties noted above), the Commission mandate by means of a further future addition to Rule 22.919, that then current ongoing manufacture of all cellular sets which have been previously type approved are manufactured only with authentication incorporated at the factory. Exemptions could be given for only those types of sets which the manufacturer can show are technologically incompatible with such an upgrade. However, I frankly do not expect to find any current production cellular phones which are incompatible with an authentication upgrade. Since authentication requires some additional non-volatile memory for such data as the A-key, SSD-A, etc., it is possible that such an upgrade in some cases will reduce the number of memory locations available for such features as stored speed-dialing numbers or other non-authentication related features. If only non-essential features like this are slightly reduced in this way, this alone should not be an acceptable reason to exempt a set type from being upgraded for authentication in continued manufacture.

13.d Three specific classes of exemptions from the general prohibition on changing the ESN are desirable now:

13.d.1 An exemption for the case of a separable chip implementation of the authentication algorithm, which chip incorporates the ESN and which is designed by the manufacturer to be moved from set to set. In this case, there should be no explicit or implicit prohibition on possession and use, by a single valid cellular customer, of multiple cellular sets and/or chips having the same MIN/ESN/A-key and related authentication data, but I agree with the comments of several others that a reasonable limit on the number of such emulated extensions should be mandated by the commission for administrative convenience I believe that the limit on landline extensions in part 68 on a single subscriber line is 12, as a starting point for discussion.

Comment: Note that the legal permission for such a move or copy of the identification incorporates the case of a chip on a chip carrier, or a chip packaged in a "smart card." The special case of replacement of a non-functioning set of this type is covered by removing the chip or smart card from the old to the new set. This changeout of the separable authentication chip is the standard procedure used in the European GSM system for the purposes of repair and upgrade, and also for rental of a cellular set for a short term, use of a semi-public GSM cellular radio in a taxicab, etc. Note that in this implementation the ESN is now in the chip and does not remain in the cellular set, unlike earlier technology and unlike paragraph 13.d.2.

It is also desirable, for a cellular phone having authentication, and particularly when the ESN is in a separable chip and not in the remaining portion of the cellular phone, to mandate a separate unique physical equipment identifier, distinct from the ESN. I suggest a physical equipment identifier, initially installed in the cellular phone's non-volatile memory at the factory, which can be remotely determined over the radio by the cellular network via a special interrogation message, because this is already done successfully in the European GSM system. However, the industry standards committees should determine the final form of this particular identifier, since other methods have value as well. This physical equipment identifier is not in the separable chip. It is not desirable to unconditionally prohibit changing this physical equipment identifier, since changing it facilitates repair and upgrading, and in any case it has absolutely no relationship to authentication or fraud. It is important for tracking stolen cellular phones or repair-related identification, so its alteration in connection with theft or unauthorized use of a cellular phone should be prohibited. However, if a manufacturer or a third party upgrades the software in the cellular phone legitimately, this is a desirable instance to change the physical equipment identification number to allow systems to automatically determine the capabilities of the cellular phone from its physical equipment identifier, which has a number of network-wide benefits.

13.d.2 An exemption for a phone in which there is no separable chip authentication but instead a "one-piece" call processing and authentication implementation, or a phone in which there is call processing but no initial factory provided authentication, and when all of such sets involved in the transfer or copying of the ESN are owned by the same valid cellular customer, and one of these retains its original ESN value. As in the previous paragraph, there should be no explicit or implicit prohibition on possession and use of multiple cellular sets having the same MIN/ESN by a single valid cellular customer, with some maximum set by the Commission. Note that this exemption also covers changing the ESN of a set to repair, replace or upgrade it, and this should be explicitly mentioned in Rule 22.919. In addition to changing the ESN in a secondary cellular phone to match the customer's primary phone for use as an extension, the Commission should explicitly recognize the changing of the ESN in the customer's cellular phone when that customer is the victim of cloning, but wishes to retain the original directory number (MIN) and change the phone's ESN only.

Comment: I agree with several petitioners that the commission should establish appropriate procedures to control who is permitted to do this type of change (the so-called "emulators") and under what conditions what type of records are kept, and to define the responsibilities of such emulators.

The particular acceptable technological methods for changing and controlling propagation of the ESN in this case (e.g. encrypted transfer, erase-before-write, central data base, etc.) and the responsibilities of persons and firms engaging in such operations (e.g., identification of who is permitted to make such changes in ESN, maintaining a central data base to prevent duplicate ESN values from being assigned, copying the ESN from a non-functioning set to a good set for use by the same valid cellular customer, etc.) should be specified.

In addition, I most strongly recommend that as soon as it is feasible, all sets which have their ESN changed in this way are also mandated to have authentication software added as well. Some reasonable calendar target should be set to allow for development and testing of the upgrade software. Specific types of sets could be exempted only if authentication is already installed, or if the manufacturer can show that the set is technologically incompatible with such an upgrade, or if the manufacturer makes such an upgrade available directly at a reasonable and competitive cost to the customer in the case that the manufacturer chooses to restrict the alteration of the software by others as a result of copyright or other special rights to the software. No manufacturer should be permitted to restrict or prevent authentication upgrade of upgradeable sets by asserting copyright or other legal rights, unless they make such a software/firmware authentication upgrade available directly to the consumer at reasonable and competitive cost. The Commission should also consider a completely separate rule mandating that any cellular phone which is repaired for any reason must also have authentication added as well.

As in section 13.d.1, a separate physical equipment identifier is desirable for theft tracking or repair related identification, and the rule should mandate installing such a number, and the software to permit remotely reading it. This same rule should apply equally to both emulated extension phones and MUSDN extension phones as well. (See comments above at the end of section 2)

13.d.3 An exemption for cellular band equipment such as BellSouth Cellemetry ®, in which the value of the ESN is changed solely to report remote measurement data, provided that the possession and use of such a cellular phone is restricted to a valid cellular customer and the cellular phone is not manufactured nor modified so that it is capable of transmitting via or utilizing a voice or traffic channel.

Oath: I declare under penalty of perjury that the facts set forth in this letter are true according to the best of my knowledge, information and belief

Respectfully submitted,

Richard C. Levine

Original to Ms. Michele Farquhar, FCC
7 copies to Secretary of FCC
Copies to petitioners: AT&T Wireless Systems,
CTIA; MT Communications

Attachment: Appendix A- BellSouth Cellemetry (4 pages)®

Cellemetry^{sm}

Thomas F. Evans

Network Access Strategy
BellSouth Wireless, Inc.
1100 Peachtree Street NE, Room 808
Atlanta, Georgia 30309

Abstract

Cellemetry^{sm} provides the means of collecting, sorting and routing short telemetry-like messages via the standard cellular telephone system. At no time does the Cellemetry^{sm} system impose any significant capacity restraints on the cellular telephone system.

Cellemetry^{sm} is applicable to a myriad of business requirements, literally any business which requires one-way or two-way short message capabilities, such as utility meter reading, alarm panel reporting, vending machine status reporting, etc. Cellemetry^{sm} provides an inexpensive means to obtain information which heretofore was obtained by manual device reading or simply was not gathered at all.

Cellemetry^{sm} uses the overhead control channels on the cellular telephone system to convey its messages in either direction. The overhead control channels are used to deliver all of the messages between the cellular telephone base station and the customer's cellular telephone. These messages are required to initiate cellular calls and maintain contact with the cellular telephones. The message handling capability of these control channels is far greater than is needed to maintain the cellular telephone call traffic, even in the busiest of times during the day. Cellemetry^{sm} makes use of this excess control channel capacity to route its messages.

Cellemetry^{sm} RADios (CRADs) imitate cellular roamer telephones. A roamer telephone is defined as one which is operating outside of its home cellular system. Each cellular system sends a message at regular intervals to all of the roamers operating in its system, telling them how to operate as a roamer. One of the requirements as a roamer is to autonomously register (AR), during which time the cellular telephone reports its mobile identity number (MIN) and electronic serial number (ESN) to the cellular system via the Reverse Control Channel. The cellular system processes this MIN and ESN and routes them via a special network back to the cellular customer's home cellular system which validates the customer's identity and provides all of the customer's calling features. This action is an effort to reduce fraudulent calls as well as provide full calling capabilities even when a customer is roaming. The Cellemetry^{sm} gateway is connected to this intra-system network and since all of the Cellemetry^{sm} MINs will be specially assigned, the Cellemetry messages are routed only to the Cellemetry^{sm} gateway.

The Cellemetry^{sm} gateway processes the Cellemetry^{sm} messages according to their type. Some are processed immediately and passed on to the customer (alarm monitoring), while others are stored and delivered to the customer in a batch (utility meter reading). The gateway also handles billing for the Cellemetry^{sm} service.

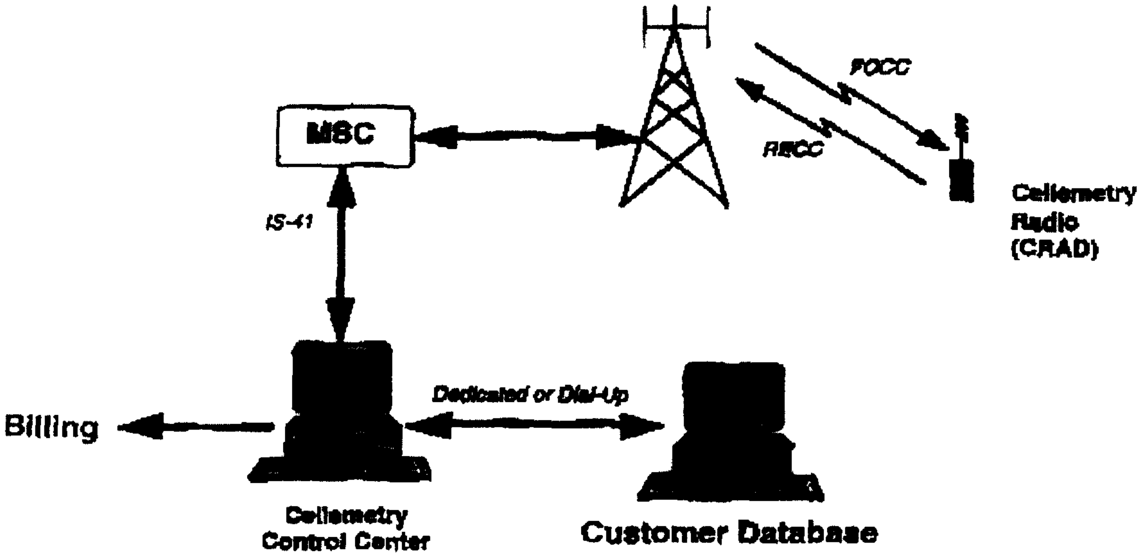

Figure 1. Cellemetry℠ Architecture.

Two data elements which are conveyed via the control channels are the Mobile Identity Number, or MIN, and the Electronic Serial Number, or ESN. Cellemetry℠ uses the MIN as an account or unit identifier. The MIN is ten digits long, the same as a standard telephone number plus Area Code. The ESN is a 32 bit number which can yield over 4 billion combinations. It is the ESN which carries the Cellemetry data message. The CRAD has the capability to store a number of MINs other than its main account identifier MIN. The action that the CRAD takes depends upon the register location in the CRAD's memory of each MIN. This action will be described in detail later.

Each CRAD acts like a roamer cellular telephone to the cellular system. A roamer cellular telephone is defined as any cellular telephone operating outside of its home system. When a cellular telephone is first activated, a Station IDentity, or SID, is programmed into the telephone. Each time the telephone is turned on, the telephone compares the SID stored in its memory to the SID transmitted by the cellular operator over the FOCC. If a match occurs, indicating the customer is in their home system, nothing happens. If a match does not occur, the telephone illuminates its "ROAM" light to indicate to the customer that they are not in their home system and that roaming charges will apply to their telephone calls. Little else occurs to the cellular telephone. However, the telephone call from a roamer is treated very differently in the cellular system. It is this difference that is used to properly route the Cellemetry℠ message.

Since a cellular telephone system does not have any data on a roamer, such as whether they are a legitimate customer and have paid their bill, the cellular telephone systems have an interconnected network, called the IS-41, over which one cellular system can request information on a roamer from the roamer's home system. The home system replies back with confirmation of the roamer's identity, payment status and any custom calling features that the roamer has in its home system. The MIN is used to route the request for the roamer information via the IS-41 network.

In the case of Cellemetry℠, the MIN of the Cellemetry℠ unit is such that the cellular switch routes the MIN and ESN of the Cellemetry user to a specific port of the IS-41 network. At this port, the Cellemetry℠ Gateway is connected. Typically, the Cellemetry℠ Gateway is physically located in the busiest cell sites, there is more than enough capacity for Cellemetry℠. To further eliminate the possibility of having any impact on the cellular system, the CRAD utilizes the busy-idle bit which is sent over the FOCC. The busy-idle bit is one bit multiplexed in the FOCC data stream which indicates that the cellular base station is communicating with a cellular user. A cellular telephone will not attempt to register with the cellular base station if the busy-idle bit is set high. Only if it is set low will the cellular telephone attempt a registration. The CRAD looks at the busy-idle bit over a multi-second window. If the busy-idle bit is set high for greater than a certain percentage of the time, the CRAD will defer its registration until the busy-idle bit activity is reduced. In this manner, regular cellular customers always will obtain the control channel first.

IV. Summary

Cellemetry℠ provides for an efficient, low-cost short message service which covers the entire footprint of a cellular system with no additional equipment required at the individual cellular base station sites. It can be easily and quickly installed with no impact on the capacity of the host cellular system.